LSI Learny Society International

IA / CYBER / TECH

PROGRAMME DE FORMATION

Gestion des incidents & SOC

Organiser détection et triage.

DURÉE	PUBLIC	FORMAT
36 h	**Professionnels et apprenants concernés par le parcours ; adaptation au secteur possible.**	**Présentiel · Distanciel · Hybride**

Ce que vous allez savoir faire

- Organiser détection et triage
- Conduire les premières étapes d’investigation
- Coordonner réponse, communication et retour d’expérience

Votre formation, en un coup d’œil

Durée	36 h	**Public**	Professionnels et apprenants concernés par le parcours ; adaptation au secteur possible.
Prérequis	Positionnement / expérience professionnelle selon le niveau.	**Modalités**	Présentiel, classe virtuelle ou hybride selon la proposition.
Tarif	Sur devis - prix et modalités communiqués avant engagement.	**Délai d’accès**	Réponse initiale sous 48 à 72 h ouvrées ; démarrage selon calendrier et financement.

Objectifs pédagogiques

- Organiser détection et triage
- Conduire les premières étapes d’investigation
- Coordonner réponse, communication et retour d’expérience

Résultats attendus

À l’issue du parcours, le bénéficiaire doit pouvoir mobiliser les compétences décrites ci-dessus et les appliquer dans les exercices, simulations ou productions prévus. Les critères de réussite sont observables dans le scénario pédagogique.

Statut / certification

Action de formation professionnelle donnant lieu à une attestation de fin de formation / réalisation et à un bilan des acquis. Aucune certification RNCP/RS ni grade académique n’est inclus par défaut, sauf mention explicite dans la proposition contractuelle.

Le parcours LSI

01 Diagnostic
Niveau, besoin, contraintes.

02 Proposition
Programme, formateur, calendrier.

03 Déploiement
Présentiel, distanciel ou hybride.

04 Évaluation
Acquis, attestation et bilan.

Programme détaillé

Chaque séquence est conçue pour produire un apprentissage observable. Les cas, exemples et outils peuvent être contextualisés au secteur du client sans réduire les objectifs ni la durée contractualisée.

Cours 1 · 6 h · SOC, SIEM, alertes, logs et niveaux de criticité

Objectif du cours : Analyser et traiter « SOC, SIEM, alertes, logs et niveaux de criticité » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - SOC, SIEM, alertes, logs et niveaux de criticité Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H2	Contrôle - sources de logs Comprendre sources de logs, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - SIEM / cas d'usage de détection Comparer SIEM et cas d'usage de détection dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H4	Lab / logs - faux positifs Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Exercice table-top - escalade Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Cours 2 · 6 h · Triage

Objectif du cours : Analyser et traiter « Triage » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - Triage Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H2	Contrôle - sources de logs Comprendre sources de logs, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - SIEM / cas d'usage de détection Comparer SIEM et cas d'usage de détection dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H4	Lab / logs - faux positifs Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Exercice table-top - escalade Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Cours 3 · 6 h · Réponse

Objectif du cours : Analyser et traiter « Réponse » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - Réponse Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H2	Contrôle - sources de logs Comprendre sources de logs, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - SIEM / cas d'usage de détection Comparer SIEM et cas d'usage de détection dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H4	Lab / logs - faux positifs Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Exercice table-top - escalade Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Cours 4 · 6 h · Communication de crise, escalade et responsabilités

Objectif du cours : Analyser et traiter « Communication de crise, escalade et responsabilités » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - Communication de crise, escalade et responsabilités Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H2	Contrôle - sources de logs Comprendre sources de logs, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - SIEM / cas d'usage de détection Comparer SIEM et cas d'usage de détection dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H4	Lab / logs - faux positifs Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Exercice table-top - escalade Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Cours 5 · 6 h · Table-top exercise ransomware / compromission

Objectif du cours : Analyser et traiter « Table-top exercise ransomware / compromission » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - Table-top exercise ransomware / compromission Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H2	Contrôle - sources de logs Comprendre sources de logs, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - SIEM / cas d'usage de détection Comparer SIEM et cas d'usage de détection dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H4	Lab / logs - faux positifs Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Exercice table-top - escalade Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Cours 6 · 6 h · Approfondissement et mise en pratique

Objectif du cours : Analyser et traiter « Approfondissement et mise en pratique » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - Approfondissement et mise en pratique Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H2	Contrôle - sources de logs Comprendre sources de logs, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - SIEM / cas d'usage de détection Comparer SIEM et cas d'usage de détection dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H4	Lab / logs - faux positifs Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Exercice table-top - escalade Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Modalités pédagogiques et qualité

Méthodes mobilisées

- Positionnement initial et contextualisation aux situations de travail du bénéficiaire.
- Apports ciblés, démonstrations, exercices guidés et entraînement progressif.
- Mises en situation, études de cas, simulations ou productions concrètes selon le domaine.
- Feedback du formateur, correction par critères observables et plan de progression.
- Ressources numériques / LMS lorsque prévues dans le scénario pédagogique.

Moyens pédagogiques et techniques

- Supports formateur, fiches de travail, études de cas et ressources décrites dans le scénario pédagogique.
- En distanciel : visioconférence et espace numérique / LMS ; ordinateur, connexion internet, micro et audio requis côté bénéficiaire.
- Assistance technique et pédagogique appropriée pendant les séquences à distance ; les activités et leurs durées sont indiquées dans le parcours.
- En présentiel : salle adaptée, accès aux supports, outils de projection et connexion lorsque les exercices le nécessitent.

Suivi de l’exécution

- Feuilles d’émargement ou traces de connexion selon la modalité.
- Productions, quiz, exercices, simulations et/ou dépôts LMS servant de preuves d’activité.
- Suivi des absences et échanges avec le bénéficiaire / commanditaire lorsque nécessaire.

Évaluation des acquis

mise en situation ou livrable final évalué avec grille de critères et plan de progression.

- Positionnement ou diagnostic initial lorsque le niveau de départ conditionne le parcours.
- Évaluations formatives pendant les cours et feedback correctif.
- Évaluation finale par test, étude de cas, simulation, production ou examen blanc selon la formation.
- Bilan des acquis communiqué au bénéficiaire ; attestation de fin de formation / réalisation.

Indicateurs de résultats

Indicateurs spécifiques à cette référence : données historiques non consolidées dans le référentiel au 05/09/2026. LSI suit a minima l’assiduité, la satisfaction, l’atteinte des objectifs et, lorsqu’un examen externe est préparé, le résultat communiqué par les candidats. Les indicateurs sont publiés dès qu’un volume de cohortes permet une lecture pertinente.

Accès, organisation et accessibilité

Modalités d’accès	Prise de contact -> diagnostic / positionnement -> proposition pédagogique et financière -> validation administrative -> planification.
Délai d’accès	Réponse initiale sous 48 à 72 h ouvrées annoncée par LSI. Le délai réel jusqu’au démarrage dépend des disponibilités, du financement et du calendrier convenu.
Horaires / calendrier	Dates, horaires et rythme détaillés communiqués dans la proposition, la convention ou la convocation avant inscription définitive.
Formateur(s)	Sélectionnés selon expertise métier / linguistique et expérience pédagogique. Identité et éléments utiles communiqués avant inscription définitive.
Accessibilité handicap	Besoins d’aménagement recueillis dès le diagnostic. Adaptations pédagogiques, techniques ou organisationnelles étudiées ; orientation vers un partenaire compétent si nécessaire.
Contact	Marcus Détrez - Fondateur LSI Education - marcus@lsi-education.com - lsi-society.com/contact
Tarif / règlement	Sur devis. Modalités de règlement dans le devis ou la convention. Les conditions financières applicables aux personnes physiques finançant elles-mêmes leur formation sont remises avant engagement.
Règlement intérieur	Le règlement intérieur applicable à la formation est mis à disposition avant inscription définitive.
Référent commanditaire	Pour les formations commandées par une organisation, les coordonnées de la personne chargée des relations avec les stagiaires côté commanditaire figurent dans les documents de session.

À FINALISER AVANT USAGE CONTRACTUEL	Identité juridique complète, SIRET, NDA, référent handicap nominatif si distinct, calendrier de session, formateurs affectés et tarifs chiffrés. Ces données ne sont pas inventées dans la plaquette.

Cadre de référence

- Code du travail, art. L6353-8 : informations mises à disposition avant inscription définitive.
- Code du travail, art. D6353-1 : mentions applicables aux conventions de formation.
- Code du travail, art. D6313-3-1 : exigences spécifiques aux actions réalisées en tout ou partie à distance.
- Référentiel national qualité - Guide de lecture Qualiopi, critère 1 / indicateur 1.
- Cette plaquette ne remplace pas le devis, la convention/contrat, la convocation ni le règlement intérieur.

POUR ALLER PLUS LOIN

Catalogue LSI
Programmes, parcours et demande de devis :
lsi-society.com/formations